OIPE IAP45
MAY 1 6 2006
PATENT & TRADEMARK OFFICE

PTO/SB/33 (07-05)
United States Patent & Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) 59643.00075
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on ______________________________ Signature ______________________________ Typed or printed Name ______________________________	Application Number: 09/924,863 Filed: August 8, 2001
	First Named Inventor: Huima ANTTI
	Art Unit: 2684 Examiner: Gesesse, Tilahun

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

____
Signature

□ Applicant/Inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under
37 CFR 3.73(b) is enclosed

David E. Brown
Typed or printed name

☒ Attorney or agent of record.
Registration No. 51,091

(703) 720-7883
Telephone number

□ Attorney or agent acting under 37 CFR 1.34.
Reg. No. is acting under 37 CFR 1.34 __________

May 16, 2006
Date

NOTE: Signatures of all of the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

□ *Total of _____ forms are submitted.

O I P E
IAP45
MAY 1 6 2006
PATENT & TRADEMARK OFFICE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

May 16, 2006

In re the Application of:

Huima ANTTI

Art Unit: 2684

Application No.: 09/924,863

Examiner: Gesesse, Tilahun

Filed: August 8, 2001

Attorney Dkt. No.: 59643.00075

For: METHOD OF SECURING COMMUNICATION

This is a Pre-Appeal Brief Request for Review from the final rejection set forth in an office action dated November 16, 2005, ("the office action") finally rejecting claims 33-42 and 58-68, and objecting to claims 43-57.

The cited references fail to disclose or suggest all of the limitations of any of the pending claims. Thus, the Final Office Action did not establish prima facie obviousness in rejecting the pending claims, which constitutes clear error.

The Office Action rejected claims 33-42 and 58-68 under 35 U.S.C. 103(a) as being obvious over U. S. Patent No. 5,642,401 to Yahagi (Yahagi), in view of U.S. Patent No. 5,991,407 to Murto (Murto). The Office Action took the position that Yahagi discloses all of the features recited in the above-identified claims except the feature of a plurality of messages selected from a set of message types, and asserts that Murto discloses this feature. This rejection is respectfully traversed.

Claim 33, upon which claims 34-62 depend, recites a method of securing communication between a first party and a second party in a telecommunications network. The method includes the step of defining acriteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method also includes the steps of selecting one of the plurality of different security methods in accordance with defined criteria and performing the security method.

Claim 63 recites a telecommunications network element for securing communication between a first party and a second party. The network element includes means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The network element also includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria and means for insuring that the communication between the first and second parties is in accordance with the selected security method.

Claim 64 recites a terminal for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The terminal further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 65 recites a system for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The system further includes a selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 66 recites a computer program product comprising computer-readable code, the computer-readable code causes a computer to perform a procedure for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The computer code further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between said first and second party is in accordance with said selected security method.

Claim 67 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method further includes selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

Claim 68 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common, selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

According to embodiments of the present invention, the first party and second party may be a mobile station and a base station. The set of message types may include messages such as random number messages, hash function messages, signature function messages, parameters for use with function messages, security parameter messages, keys for function messages, encoded messages, messages to and/or from a third party and authentication response messages. These are all particular message types that may be used in authenticating a mobile station for use in a communication network. Thus, it is possible to select from a large number of different security methods. It is respectfully submitted that the claimed invention advantageously allows a relatively large number of different security methods to be implemented using only a small number of different messages. As shown at least in Figures 3 – 9, the claimed invention includes a plurality of different security methods. Accordingly, independent claims 33 and 63-68 recite the feature of selecting a security method from a plurality of security methods.

Yahagi is directed to an authentication method whereby a base station authenticates a mobile station. The method include selecting a random number RAND(j) and corresponding authentication calculations are made from a plurality of parameters RAND(1...n) and SRES(1...n) respectively (for example, see column 2 lines 1-13 of Yahagi). The method further includes a method key Ki that is specific to the mobile station being authenticated (for example, see column 4 lines 18-23 of Yahagi).

Murto is directed to an authentication method whereby each subscriber is allocated an IMSI (International Mobile Subscriber Identity) number, a subscriber authentication key Ki, a plurality of "triplets" (Kc, RAND, SRES) for use in authenticating that subscriber (for example, see column 1 lines 37-55 of Murto). Each value of SRES and Kc is calculated based on Ki and a respective value of RAND (for example, see column 1 lines 49-53 of Murto).

Applicant respectfully submits that the cited references, individually or combined, fail to disclose or suggest at least the feature of defining criteria for selecting one of a plurality of different security methods, as recited in claim 33 and similarly recited in claims 63-68. This deficiency constitutes clear error in the Office Action.

Instead, Yahagi discloses an "authentication algorithm calculation means 6 [that] performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters" (column 3, lines 63-67). In Figure 3 thereof, Yahagi further discloses the steps of a single authentication method. The single method disclosed in Yahagi merely selects a random number from a plurality of random numbers. Regardless of which random number is chosen, the same authentication method is used because the use of different random numbers merely changes the parameters of the single authentication method. The Office Action alleged that the values RAND (1...n) and SRES(1...n) of Yahagi can be interpreted as a plurality of method steps. However, Yahagi (col. 2 lines 7-24) merely discloses a single security method, which is a function of a random number. Therefore, the same method is used regardless of which of the parameters are utilized in the authentication method. Thus, any reasonable interpretation of Yahagi will have to show how a different method is used for authentication, regardless of the values of the random parameters, RAND.

The Office Action admits that Yahagi does not disclose the feature of a plurality of messages selected from a set of message types and alleges that Murto cures this deficiency.

Murto discloses an authentication procedure in a GSM-based mobile communications system. The Office Action relies on Murto to disclose the feature of a plurality of messages selected from a set of message types. Murto, similar to Yahagi, discloses a GSM authentication method involving selecting a random number RAND from a plurality of random numbers RAND(1…n) and calculating a respective authentication result SRES. As discussed above, the method of Murto includes selecting one of a plurality of "triplets" each comprising a random number RAND, an authentication result SRES and a ciphering key Kc (see column 5 lines 35-45 of Murto). These triplets are derived using pairs of values IMSI and Ki, (alleged plurality of message types). Thus, Murto only discloses a single message and does not disclose or suggest a plurality of messages, as alleged in the Office Action. This deficiency constitutes clear error in the Office Action because Murto fails to cure the admitted deficiencies of Yayagi.

Based at least on the above, Applicant respectfully submits that the cited references fails to disclose or suggest all of the features recited in any of the pending claims. Thus, the failure to establish prima facie obviousness constitutes clear error in the Office Action.

Conclusion

For all of the above noted reasons, it is strongly submitted that certain clear differences exist between the present invention and the prior art relied upon by the Examiner and that a *prima facie* case of obviousness has clearly not been established. This final rejection being in clear error, therefore, it is respectfully requested that the Examiner's decision be reversed in this case regarding the rejection of claims 33-42 and 58-68, and objecting to claims 43-57, and that this application be passed to issue.

Respectfully submitted,

David E. Brown, Attorney for Applicant
Registration No. 51,091

Customer Number 32294
SQUIRE, SANDERS & DEMPSEY LLP
8000 Towers Crescent Drive, 14th Floor
Tysons Corner, VA 22182-2700
Tel: (703) 720-7800/ Fax (703) 720-7802
DEB:jkm

Encl.: Notice of Appeal
Form PTO/SB/33
Check No. 14470